UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/923,727	08/06/2001	Randy Keith Lomnes	470039.401	1112

500 7590 11/30/2006

SEED INTELLECTUAL PROPERTY LAW GROUP PLLC
701 FIFTH AVE
SUITE 5400
SEATTLE, WA 98104

EXAMINER	
TSAI, SHENG JEN	

ART UNIT	PAPER NUMBER
2186	

DATE MAILED: 11/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/923,727	LOMNES, RANDY KEITH	
	Examiner	Art Unit	
	Sheng-Jen Tsai	2186	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 October 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,11,13-54,56-81 and 83* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9,11,13-54,56-81 and 83* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is taken in response to Applicants' Amendments and Remarks filed on October 26, 2006 regarding application 09,923,727 filed on August 6, 2001.

2. Claims 10, 12, 55 and 82 have been cancelled previously.

Claims 28, 51 and 69 have been amended.

Claims 1-9, 11, 13-54, 56-81 and 83 are pending for consideration.

3. ***Response to Remarks and Amendments***

Applicants' remarks have been fully and carefully considered with Examiner's response set forth below.

Withdrawal of claim rejections under 35 USC 112

Applicants have amended claims 28 and 51 to clarify that the limitations of "copying the saved data from the redirected space to associated locations in the protected space" is performed after the restart of the computer system. This amendment eliminates the inconsistency between claims 28 and claim 3, as well as between claim 51 and 32. Therefore, the rejections of claims 28 and 51 under 35 USC 112, second paragraph have been withdrawn.

Applicants also provide explanations to clarify that the limitations recited in claims 67 and 69 are not inconsistent with each other. As such, the rejection of claim 69 under 35 USC 112, second paragraph has also been withdrawn.

Response to Remarks on reference Hansen regarding claims 1-3, 32, 54, 72 and 79

Each of claims 1-3, 32, 54, 72 and 79 recites the limitation of "... **access request that would otherwise modify a portion of data on the storage device**, ..."

Applicant contends that Hansen et al. (US 5,832,263) do not teach this particular limitation, and that the Examiner made improper interpretations on Hansen's teachings. The Examiner disagrees with this assessment for the following reasons.

First, the invention of Hansen et al. is directed to storage media where access is artificially imposed as an access control method [For example, on a network running under the UNIX operating system, file and directory access privileges may be restricted to a designated user list to control access to the information. Such files or directories appear to be non-modifiable or read-only stores of information to those users or agents (such as other programs, daemons, systems, or the like) which do not possess the appropriate privileges (column 1, lines 17-23); As used herein, "non-modifiable store (NMS)" refers to any storage which does not allow information or data to be changed whether this limitation is imposed by a physical constraint of the storage media or artificially imposed as an access control method (column 3, lines 49-53)].

Note that for storage media where access is artificially imposed as an access control method, the storage only appears to be non-modifiable to those users who do not have the appropriate privileges. In other words, for those users with appropriate privileges, access (i.e., read and write) to the storage is not restricted at all and the storage is modifiable.

Second, the Examiner only relies on the type of storage media where access is artificially imposed as an access control method, and is modifiable to those users with

appropriate privileges, as mentioned by Hansen et al. for teaching the limitations recited in the claims. The Examiner does not rely on the type of storage media that is not modifiable due to physical restrictions, such as CD-ROM, for teaching the limitations recited in the claims.

Third, it is well known in the art that, in order to restrict access only to users having the appropriate privileges, any access to the storage has to be intercepted and interrogated to ensure that the access is requested by a designated user with the appropriate privileges [For example, on a network running under the UNIX operating system, file and directory access privileges may be restricted to a designated user list to control access to the information (column 1, lines 17-23)].

Fourth, since designated users of the appropriate privileges are allowed to access (i.e., read and write) to the information, modification would still occur when privileged users write into the storage space, intentionally or inadvertently, regardless whether unauthorized users may also alter the contents of the storage device through hacking.

Therefore, the Examiner's position regarding the status of these claims, and those claims depending from them, remains the same as stated in the previous Office Action.

Response to Remarks on reference White regarding claims 1-3, 32, 54, 72 and 79

Applicants contend that reference White et al. (US 6,092,161) do not teach the limitation of a redirect driver or other software components installed or loaded into

memory, because White et al. only describe hardware and firmware, but not software. The Examiner disagrees with this assessment for the following reasons.

First, Applicants are correct in stating that the invention of White et al. comprises firmware component [Alternatively, the apparatus may provide firmware means adapted to be incorporated into the computer system (column 5, lines 30-31)].

Second, it is well known in the art that firmware is a special type of software. For example, Microsoft Computer Dictionary defines the term "firmware" as "software routines stored in read-only memory (ROM)" [Microsoft Computer Dictionary, 5th edition, Microsoft Press, isbn 0-7356-1495-4, page 215]. Thus, contrary to Applicants' argument, the invention of White et al. indeed includes software components.

Third, the program flow chart in figure 2 of White et al. shows the first step of determining "Has area 'A' already been changed this session?" followed by the second step of "find free sectors in Virus Isolator Space or within a Dormant Partition" if the answer to the first step is a "no." Note the action of "find free sectors in Virus Isolator Space or within a Dormant Partition" is a redirection to direct requested modifications/changes to the designated space [figure 2]. Figure 5 provides another example of this redirection paradigm.

Therefore, the Examiner's position regarding the status of these claims, and those claims depending from them, remains the same as stated in the previous Office Action.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-9, 11, 13-15, 30, 32-40, 50, 52-64, 66, 71-72, 74, 76-79, 81 and 83 are rejected under 35 U.S.C. 102(b) as being anticipated by Hansen et al. (U.S. 5,832,263).

As to claim 1, Hansen et al. disclose **a method in a computer system for automatically protecting data stored on a storage device from alteration** [It is a further object of the present invention to provide a system and method for modifying information recorded in a non-modifiable store (figure 3, 44) by intercepting file accesses and redirecting them based on whether originally stored information has been updated (column 2, lines 17-21); since the modifying information is always directed to another designated area (the tracking store, figure 3, 46), the data of the designated protected area (figure 3, 44) is automatically protected from alteration as modifications is applied to another designated area (the tracking store, figure 3, 46)], **the computer system having an operating system** [column 4, lines 43-51], **redirection driver code** [the corresponding redirection driver comprises the Information Retriever/Modifier (Agent) (figure 3, 48), the In-Place Modifier (figure 3, 42), the Non-Modifiable Store (figure 3, 44) and the Tracking Store (figure 3, 46); figures 1 and 2 show the flow diagrams of the redirection driver code; column 2, lines

58-65], **available storage and redirected storage** [the Non-Modifiable Store (figure 3, 44) and the Tracking Store (figure 3, 46); column 5, lines 30-50; column 5, lines 65-67; column 6, lines 1-30], **comprising**:

Starting the computer system from a first powered-down state, wherein the data stored in a plurality of original locations on the storage device is in an original state [the Non-Modifiable Store (figure 3, 44) contains read-only data that is never changed from its original state because it is read-only];

Loading the redirection driver code into a memory of the computer system [column 2, lines 58-65; column 5, lines 51-64];

receiving a request for write access that would otherwise modify [refer to "***As to Amendments and Remarks on claims 1-3, 32, 54, 72 and 79***" presented earlier in this Office Action] **a portion of data on the storage device, the request referring to one of the original locations on the storage device** [abstract; column 2, lines 17-21; column 4, lines 27-42] ;

under control of the loaded redirection driver [the Information Retriever/Modifier (Agent) (figure 3, 48) and the In-Place Modifier (figure 3, 42); column 5, lines 51-67; column 6, lines 1-30],

intercepting the request for write access to the data [the method and system intercepts read and write requests targeted at the read-only storage (abstract; column 2, lines 17-22); figure 2];

determining whether the request refers to the one of the original locations [the Non-Modifiable Store (figure 3, 44)] **that has previously been redirected to**

redirected storage [the Tracking Store (figure 3, 46)] **when the request refers to an original location that has previously been redirected to redirected storage, using a location in redirected storage as a current redirected location** [figure 1], **otherwise allocating available storage to a new location in redirected storage and using the new location as the current redirected location** [figure 2]; **and redirecting the access request to refer to the current redirected location, such that the request transparently accesses the current redirected location instead of the original location** [figures 1 and 2]; **and**

restarting the computer system from a second powered-down state, wherein the data stored in the plurality of original location on the storage device automatically remains unaltered from the original state, without any restorative copying of data to the plurality of original locations [since the modifying information is always directed to another designated area (the tracking store, figure 3, 46), the data of the designated protected area (figure 3, 44) is automatically protected from alteration as modifications is applied to another designated area (the tracking store, figure 3, 46)].

Further, claims 32, 54, 55, 72, 79, and 83 are rejected due to the same reasoning as provided in "As to claim 1."

As to claim 2, Hansen et al. disclose **a computer system for automatically protecting data stored on a storage device from alteration, the data stored in a plurality of original locations on the storage device and in an original state when**

the computer system is started from a first powered-down state [refer to "As to claim 1"], **comprising**:

data access request that would otherwise modify an original location on the storage device [refer to "As to claim 1," abstract; column 2, lines 17-22];

available storage [refer to "As to claim 1"]; **and**

redirection driver, installed in the computer system during power-up initialization [refer to "As to claim 1"], **that,**

automatically intercepts the data access request [refer to "As to claim 1"]; **and redirects the access request to access a redirected location in the available storage, such that a requested modification at the original location is not performed and is instead performed to the redirected location, and such that, when the computer system is restored from a second powered-down state, the data in the original location on the storage device automatically remains unaltered from the original state without any restorative copying of data to the plurality of original locations** [refer to "As to claim 1"].

As to claim 3, Hansen et al. disclose **a method in a computer system for using software loaded into memory during power-up initialization to automatically protecting data stored in a portion of a storage device** [refer to "As to claim 1," figures 1 and 2; column 4, lines 43-51; column 5, lines 51-67; column 6, lines 1-30] **having a designated protected space** [the Non-Modifiable Store (figure 3, 44)], **the computer system having a redirected space** [the Tracking Store (figure 3, 46)], **comprising**:

Under control of the loaded software [refer to "As to claim 1," figures 1 and 2; column 4, lines 43-51; column 5, lines 51-67; column 6, lines 1-30]; **intercepting from requesting code a request that would otherwise modify a location in the protected space of the storage device** [refer to "As to claim 1"]; **and determining a location in the redirected space that is associated with the location in the protected space** [refer to "As to claim 1"]; **and redirecting the intercepted request to modify the determined location in the redirected space instead of the location in the protected space, in a manner that is transparent to the requesting code** [the modifying information may appear to the user to ... (abstract)], **so that the data stored in the location in the protected space automatically remains unaltered when the computer system is restarted from a powered-down state** [refer to "As to claim 1"].

As to claim 4, refer to "As to claim 3" and "As to claim 1."

As to claim 5, Hansen et al. disclose that **the driver is inserted into a driver hierarchy that is controlled by an operating system of the computer system** [column 4, lines 43-51].

As to claim 6, Hansen et al. teach that **the designated protected space of the storage device comprises the entire storage device** [the Non-Modifiable Store (figure 3, 44) may comprises as a ROM or any other read-only device, and the entire device is read-only (abstract)].

As to claim 8, Hansen et al. teach that **the determined location in the redirected space resides in another storage device** [the Tracking Store (figure 3,

46) may be a RAM (column 1, lines 48-65) that is separated from the NMS; the NMS and TS both may be implemented with removable media (column 5, lines 30-50)].

Further, claims 33, 35, and 58 are rejected due to the same reasoning as provided in "As to claims 6 and 8."

As to claim 7, Hansen et al. teach that **the determined location in the redirected space resides in the storage device** [the NMS and TS both may be a permanent part of the storage system (column 5, lines 30-50)].

Further, claims 34 and 59 are rejected due to the same reasoning as provided in "As to claim 7."

As to claim 9, Hansen et al. teach **the method of claim 3. further comprising**: **intercepting from requesting code a request to read the location in the protected space of the storage device** [figures 1 and 2, abstract; column 2, lines 17-22]; **determining the location in the redirected space that is associated with the location**
in the protected space [figures 1 and 2; column 3, lines 62-67; column 4, lines 1-15]; **and**
automatically redirecting the intercepted request to read from the determined location in the redirected space instead of from the location in the protected space in a manner that is transparent to the requesting code [figures 1 and 2; column 5, lines 51-67; column 6, lines 1-30].

Further, claims 36, 60, and 81 are rejected due to the same reasoning as provided in "As to claim 9."

As to claim 11, Hansen et al. teach that **the request to access a location in the protected space is a request to write to the protected space** [the method and system intercepts read and write requests targeted at the read-only storage (abstract; column 2, lines 17-22); figure 2].

Further, claims 37, 61, and 82 are rejected due to the same reasoning as provided in "As to claim 11."

As to claim 38, refer to "As to claim 1."

As to claim 13, Hansen et al. teach **the redirecting the intercepted write request results in automatically allocating available space to use as new redirected space and writing data to a location in the new redirected space** [figure 2; column 5, lines 51-67; column 6, lines 1-30].

As to claims 14 and 39, Hansen et al. teach **the determining the location in the redirected space that is associated with the location in the protected space further comprises first allocating available space to be used as the redirected space** [figure 2; column 5, lines 51-67; column 6, lines 1-30].

As to claims 15, 40, and 62, Hansen et al. teach that **the storage device is one of a hard disk drive, a read/write CD ROM drive, a floppy disk drive, and a semi-persistent storage device** [column 3, lines 46-60; column 1, lines 40-65].

As to claim 30, Hansen et al. teach **using redirection tables to associate locations in the protected space to locations in the redirected space** [tables are used to map and track modified areas within MNS (column 4, lines 66-67; column 5, lines 1-11; column 5, lines 51-67; column 6, lines 1-30)].

As to claim 32, refer to "As to claim 1."

As to claim 50, refer to "As to claim 27."

As to claim 52, refer to "As to claim 29."

As to claim 53, refer to "As to claim 30."

As to claim 54, refer to "As to claim 1."

As to claim 56, refer to "As to claim 30."

As to claim 57, refer to "As to claim 27."

As to claim 58, refer to "As to claim 8."

As to claim 59, refer to "As to claim 7."

As to claim 60, refer to "As to claim 1."

As to claim 61, refer to "As to claim 1."

As to claim 62, refer to "As to claim 15."

As to claim 63, Hansen et al. teach that **the redirection driver refers to the redirected storage space in at least one of files, clusters, virtual clusters, and sectors of data** [for file based system, ... (column 6, lines 1-12; column 6, lines 31-33; column 6, lines 52-67; figures 4 and 5)].

As to claim 64, Hansen et al. teach that **the redirection driver refers to the redirected storage space using multiple data addressing abstractions** [column 6, lines 52-67; figures 4 and 5].

As to claim 66, refer to "As to claim 5."

As to claim 71, refer to "As to claim 27."

As to claim 72, refer to "As to claim 1." Further, it is inherent that a driver must be installed before it is invoked in a calling sequence.

As to claim 73, Hansen et al. teach that **the redirection driver cannot be uninstalled by a user without special access privileges, thereby forcing the data to be securely maintained** [It is often desirable to modify portions of information which may be recorded in a non-modifiable store (NMS) whether this limitation is due to the physical storage media or artificially imposed by the operating system or system administrator. Modification of information may include adding, changing, or deleting portions of the information from these stores (column 1, lines 34-38); For example, on a network running under the UNIX operating system, file and directory access privileges may be restricted to a designated user list to control access to the information (column 1, lines 17-20); note that uninstalling is accomplished by deleting].

As to claim 74, refer to "As to claim 5."

As to claim 75, refer to "As to claim 5."

As to claim 76, refer to "As to claim 63."

As to claim 77, refer to "As to claim 64."

As to claim 78, refer to "As to claim 30."

As to claim 79, refer to "As to claim 1."

As to claim 81, refer to "As to claim 1."

As to claim 83, refer to "As to claim 1," "As to claim 30," and "As to claim 13."

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-4, 27-29, 32, 50-52, 54, 55, 67-69, 72, 79, and 83 are rejected under 35 U.S.C. 102(e) as being anticipated by White et al. (U.S. 6,092,161).

As to claim 1, White et al. disclose **a method in a computer system for automatically protecting data stored on a storage device from alteration** [Method and Apparatus for Controlling Access to and Corruption of Information in a Computer (title)], **the computer system having an operating system** [the supervising means causing a reset to be required of the computer system should an attempt be made to perform a prohibited read, write or format operation, said reset causing memory to be cleared and the operating system to be loaded (column 1, lines 36-39)], **redirection driver code** [figures 2-3 and 5 show the redirection program code], **available storage and redirected storage** [figure 1 shows various partitions of storage and redirected areas], **comprising**:

Starting the computer system from a first powered-down state, wherein the data stored in a plurality of original locations on the storage device is in an original state [initial connection, column 7, lines 56-67; column 8, lines 1-20];

Loading the redirection driver code into a memory of the computer system [the supervising means causing a reset to be required of the computer system should an attempt be made to perform a prohibited read, write or format operation, said reset causing memory to be cleared and the operating system to be loaded (column 1, lines 36-39)];

receiving a request for write access that would otherwise modify a portion of data on the storage device, the request referring to one of the original locations on the storage device [dividing information stored on the storage medium into a plurality of non-overlapping partitions including a boot partition and at least one general partition, characterized by: designating at least one of said partitions a Write Many Recoverable (WMR) partition wherein, in use, if a write command is issued to overwrite any resident information stored in a/the WMR partition by updating information is written on the storage medium in a location other than where the resident information is stored and a (virtual) pointer to the updated information is set up/kept so that the updated information can be accessed, as required during a remainder of a session (abstract)] ;

under control of the loaded redirection driver [figures 2-3 and 5],

intercepting the request for write access to the data [dividing information stored on the storage medium into a plurality of non-overlapping partitions including a boot partition and at least one general partition, characterized by: designating at least one of said partitions a Write Many Recoverable (WMR) partition wherein, in use, if a write command is issued to overwrite any resident information stored in a/the WMR partition

by updating information is written on the storage medium in a location other than where the resident information is stored and a (virtual) pointer to the updated information is set up/kept so that the updated information can be accessed, as required during a remainder of a session (abstract)];

determining whether the request refers to the one of the original locations [dividing information stored on the storage medium into a plurality of non-overlapping partitions including a boot partition and at least one general partition, characterized by: designating at least one of said partitions a Write Many Recoverable (WMR) partition wherein, in use, if a write command is issued to overwrite any resident information stored in a/the WMR partition by updating information is written on the storage medium in a location other than where the resident information is stored and a (virtual) pointer to the updated information is set up/kept so that the updated information can be accessed, as required during a remainder of a session (abstract)] **that has previously been redirected to redirected storage** [dividing information stored on the storage medium into a plurality of non-overlapping partitions including a boot partition and at least one general partition, characterized by: designating at least one of said partitions a Write Many Recoverable (WMR) partition wherein, in use, if a write command is issued to overwrite any resident information stored in a/the WMR partition by updating information is written on the storage medium in a location other than where the resident information is stored and a (virtual) pointer to the updated information is set up/kept so that the updated information can be accessed, as required during a remainder of a session (abstract)] **when the request refers to an original location that has**

previously been redirected to redirected storage, using a location in redirected storage as a current redirected location [figures 2-3 and 5], **otherwise allocating available storage to a new location in redirected storage and using the new location as the current redirected location** [figures 2-3 and 5]; **and**

redirecting the access request to refer to the current redirected location, such that the request transparently accesses the current redirected location instead of the original location [figures 2-3 and 5; designating at least one of said partitions a Write Many Recoverable (WMR) partition wherein, in use, if a write command is issued to overwrite any resident information stored in a/the WMR partition by updating information is written on the storage medium in a location other than where the resident information is stored and a (virtual) pointer to the updated information is set up/kept so that the updated information can be accessed, as required during a remainder of a session (abstract)]; **and**

restarting the computer system from a second powered-down state, wherein the data stored in the plurality of original location on the storage device automatically remains unaltered from the original state, without any restorative copying of data to the plurality of original locations [A system reset causes the updated information, together with the list of pointers to this information to be cleared. This returns the WMR partition to its original state as configured in Unsupervised Mode (column 2, lines 23-26)].

Further, claims 32, 54, 55, 72, 79, and 83 are rejected due to the same reasoning as provided in "As to claim 1."

As to claim 2, White et al. disclose **a computer system for automatically protecting data stored on a storage device from alteration, the data stored in a plurality of original locations on the storage device and in an original state when the computer system is started from a first powered-down state** [refer to "As to claim 1"], **comprising**:

data access request that would otherwise modify an original location on the storage device [designating at least one of said partitions a Write Many Recoverable (WMR) partition wherein, in use, if a write command is issued to overwrite any resident information stored in a/the WMR partition by updating information is written on the storage medium in a location other than where the resident information is stored and a (virtual) pointer to the updated information is set up/kept so that the updated information can be accessed, as required during a remainder of a session (abstract)];

available storage [refer to "As to claim 1"]; **and**

redirection driver, installed in the computer system during power-up initialization [figures 2-3 and 5 show the redirection driver; initial connection, column 7, lines 56-67; column 8, lines 1-20], **that,**

automatically intercepts the data access request; and redirects the access request to access a redirected location in the available storage, such that a requested modification at the original location is not performed and is instead performed to the redirected location [designating at least one of said partitions a Write Many Recoverable (WMR) partition wherein, in use, if a write command is issued to overwrite any resident information stored in a/the WMR partition by updating

information is written on the storage medium in a location other than where the resident information is stored and a (virtual) pointer to the updated information is set up/kept so that the updated information can be accessed, as required during a remainder of a session (abstract), **and such that, when the computer system is restored from a second powered-down state, the data in the original location on the storage device automatically remains unaltered from the original state without any restorative copying of data to the plurality of original locations** [A system reset causes the updated information, together with the list of pointers to this information to be cleared. This returns the WMR partition to its original state as configured in Unsupervised Mode (column 2, lines 23-26)].

As to claim 3, Hansen et al. disclose **a method in a computer system for using software loaded into memory during power-up initialization to automatically protecting data stored in a portion of a storage device** [figures 2-3 and 5 show the redirection driver; initial connection, column 7, lines 56-67; column 8, lines 1-20; the supervising means causing a reset to be required of the computer system should an attempt be made to perform a prohibited read, write or format operation, said reset causing memory to be cleared and the operating system to be loaded (column 1, lines 36-39)] **having a designated protected space** [designating at least one of said partitions a Write Many Recoverable (WMR) partition wherein, in use, if a write command is issued to overwrite any resident information stored in a/the WMR partition by updating information is written on the storage medium in a location other than where the resident information is stored and a (virtual) pointer to the updated information is

set up/kept so that the updated information can be accessed, as required during a remainder of a session (abstract)], **the computer system having a redirected space** [figure 1], **comprising**:

Under control of the loaded software [figures 2-3 and 5]

intercepting from requesting code a request that would otherwise modify a location in the protected space of the storage device [designating at least one of said partitions a Write Many Recoverable (WMR) partition wherein, in use, if a write command is issued to overwrite any resident information stored in a/the WMR partition by updating information is written on the storage medium in a location other than where the resident information is stored and a (virtual) pointer to the updated information is set up/kept so that the updated information can be accessed, as required during a remainder of a session (abstract)]; **and**

determining a location in the redirected space that is associated with the location in the protected space; and redirecting the intercepted request to modify the determined location in the redirected space instead of the location in the protected space, in a manner that is transparent to the requesting code [designating at least one of said partitions a Write Many Recoverable (WMR) partition wherein, in use, if a write command is issued to overwrite any resident information stored in a/the WMR partition by updating information is written on the storage medium in a location other than where the resident information is stored and a (virtual) pointer to the updated information is set up/kept so that the updated information can be accessed, as required during a remainder of a session (abstract)]**, so that the data**

stored in the location in the protected space automatically remains unaltered when the computer system is restarted from a powered-down state [A system reset causes the updated information, together with the list of pointers to this information to be cleared. This returns the WMR partition to its original state as configured in Unsupervised Mode (column 2, lines 23-26)].

As to claim 4, refer to "As to claim 3" and "As to claim 1."

As to claims 27-28, White et al. teach **receiving a request to shutdown the computer system; and upon receiving the request to shutdown the computer system, saving the data stored in the redirected space; wherein saving the data stored in the redirected space comprises copying the data from the redirected space to associated locations in the protected space, thereby making permanent the data that was redirected to the redirected space** [designating at least one of said partitions a Write Many Recoverable (WMR) partition wherein, in use, if a write command is issued to overwrite any information stored in a/the WMR partition prior to undertaking said write command said information is copied and stored elsewhere on the storage medium to be copied back to said WMR partition when required -- for example upon a system reset (column 3, lines 53-60)].

As to claim 29, White et al. teach **saving the data stored in the redirected space comprises saving the association between the protected space and the redirected space without copying the data from the redirected space** [the use of the WMR-SRT pointer serves this purpose (figure 1; column 2, lines 66-67; column 3, lines 1-4)].

As to claims 50-51, refer to "As to claims 27-28."

As to claims 52, refer to "As to claims 29."

As to claim 54, White et al. disclose **a computer system for protecting data stored in a portion of a storage device** [Method and Apparatus for Controlling Access to and Corruption of Information in a Computer (title)], **comprising**: **protected space designated on the storage device for storing the protected data** [dividing information stored on the storage medium into a plurality of non-overlapping partitions including a boot partition and at least one general partition, characterized by: designating at least one of said partitions a Write Many Recoverable (WMR) partition wherein, in use, if a write command is issued to overwrite any resident information stored in a/the WMR partition by updating information is written on the storage medium in a location other than where the resident information is stored and a (virtual) pointer to the updated information is set up/kept so that the updated information can be accessed, as required during a remainder of a session (abstract)]; **redirected storage space in the computer system designated for storing attempted modifications of the protected data** [designating at least one of said partitions a Write Many Recoverable (WMR) partition wherein, in use, if a write command is issued to overwrite any resident information stored in a/the WMR partition by updated information the updated information is written on the storage medium in a location other than where the/any resident information is stored and a (virtual) pointer to the updated information is set up/kept so that the updated information can be accessed, as required during a remainder of a session (column 2, lines 13-22)];

redirection driver [said supervising means allowing/restricting/prohibiting read/write operations upon the storage medium depending upon whether information to be read from a sector or written to a sector is operating system information or user information, whether the sector is in the boot partition or in a general partition, and whether the partition is active or inactive (column 2, lines 47-53)], **installed in the computer system** [Preferably according to the method of the first aspect of the present invention there is also provided supervising means (a Supervisor) separate from a central processing unit (CPU) of the computer system and made inaccessible to the user (column 2, lines 42-46)], **that intercepts requests to access locations in the protected space; redirects intercepted requests so that the requests result in accessing locations in the redirected storage space instead of locations in the protected space** [designating at least one of said partitions a Write Many Recoverable (WMR) partition wherein, in use, if a write command is issued to overwrite any resident information stored in a/the WMR partition by updated information the updated information is written on the storage medium in a location other than where the/any resident information is stored and a (virtual) pointer to the updated information is set up/kept so that the updated information can be accessed, as required during a remainder of a session (column 2, lines 13-22)], **thereby leaving the protected space unaltered** [A system reset causes the updated information, together with the list of pointers to this information to be cleared. This returns the WMR partition to its original state as configured in Unsupervised Mode (column 2, lines 23-26)].

As to claim 67, White et al. teach that **the computer system of claim 54, further comprising: unprotected space designated on the storage device for allowing modifications to a portion of the storage device** [the corresponding unprotected space is the general partition (figure 1, 4; column 3, lines 5-10); A general partition is simply a partition other than an RO or WMR partition and one which may be written to (column 6, lines 29-31)].

As to claim 68, White et al. teach that **the computer system of claim 67 wherein the redirection driver disregards access requests to the unprotected space** [the corresponding unprotected space is the general partition (figure 1, 4; column 3, lines 5-10); A general partition is simply a partition other than an RO or WMR partition and one which may be written to (column 6, lines 29-31)].

As to claim 69, White et al. teach that **the computer system of claim 67 wherein the redirection driver intercepts and redirects access requests to access locations in the unprotected space so that the access requests to the unprotected space are also redirected** [the corresponding unprotected space is the general partition (figure 1, 4; column 3, lines 5-10); A general partition is simply a partition other than an RO or WMR partition and one which may be written to (column 6, lines 29-31); designating at least one of said partitions a Write Many Recoverable (WMR) partition wherein, in use, if a write command is issued to overwrite any resident information stored in a/the WMR partition by updated information the updated information is written on the storage medium in a location other than where the/any resident information is stored and a (virtual) pointer to the updated information is set

up/kept so that the updated information can be accessed, as required during a remainder of a session (column 2, lines 13-22)].

8. ***Related Prior Art of Record***

The following list of prior art is considered to be pertinent to applicant's invention, but not relied upon for claim analysis conducted above.

- Harish et al., (US 5,940,850), "System and Method for Selectively Enabling Load-on-Write of Dynamic ROM data to RAM."
- Piazza, (U.S. 5,603,011), "Selective Shadowing and Paging in Computer Memory Systems."
- Wade et al., (U.S. 5,552,776), "Enhanced Security System for Computing Devices."
- Alexander et al., (U.S. 5,363,334), "Write Protection Security for Memory Device."
- Brant et al., (U.S. 5,848,435), "Address Protection Circuit and Method for Preventing Access to Unauthorized Address Ranges."
- Rose, (U.S. 5,144,660), "Securing a Computer against Undesired Write Operations to or Read Operations from a Mass Storage Device."
- Berglund et al., (U.S. 3,828,327), "Simplified Storage Protection and Address Translation under System Mode Control in a Data Processing System."
- Elliott et al., (U.S. 5,559,993), "Hardware Circuit for Securing a Computer against Undesired Write and/or Read operations."

- Schlotterer et al., (U.S. 3,827,029), "Memory and Program Protection System for a Digital Computer System."
- Belsan et al., (U.S. 5,193,184), "Deleted Data File Space Release System for a Dynamically Mapped Virtual Data Storage Subsystem."

Conclusion

9. Claims 1-9, 11, 13-54, 56-81 and 83 are rejected as explained above.

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sheng-Jen Tsai whose telephone number is 571-272-4244. The examiner can normally be reached on 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Matthew Kim can be reached on 571-272-4182. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Sheng-Jen Tsai
Examiner
Art Unit 2186

November 20, 2006

PIERRE BATAILLE
PRIMARY EXAMINER
11/24/06